DRN-5691336

## The complaint

Mr K complains that Wise Payments Limited ('Wise') won't reimburse him after he fell victim to a scam.

## What happened

I'll briefly set out the circumstances of the complaint, as explained by Mr K's representative.

Mr K says he saw an article online about investing through a company I'll refer to as X in this decision. He believes the investment opportunity was celebrity endorsed but cannot recall which celebrity was involved. After providing some details Mr K received a call from a representative of X. Mr K was persuaded to invest in cryptocurrency.

Mr K was advised to open accounts with Wise and with a cryptocurrency provider and linked payment facilitator I'll refer to as B. Mr K was also asked to open a further EMI account with Z. He transferred funds to Wise from a joint bank account and made payments as set out in the table below. All card payments except the first were to a cryptocurrency wallet in Mr K's own name (B). Almost all the transfers were to Z (excluding the final two – which also went to an account in Mr K's name).

| Transaction | Date | Amount | Method |
|---|---|---|---|
| 1 | 18/07/23 | £65.35 | Card |
| 2 | 27/07/23 | £300 | Card |
| 3 | 27/07/23 | £300 | Card |
| 4 | 27/07/23 | £300 | Card |
| 5 | 27/07/23 | £300 | Card |
| 6 | 27/07/23 | £300 | Card |
| 7 | 27/07/23 | £300 | Card |
| 8 | 28/07/23 | £50 | Card |
| 9 | 28/07/23 | £50 | Card |
| 10 | 31/07/23 | £90 | Card |
| 11 | 31/07/23 | £90 | Card |
| 12 | 31/07/23 | £90 | Card |
| 13 | 31/07/23 | £90 | Card |
| 14 | 31/07/23 | £205 | Card |
| 15 | 01/08/23 | £300 | Card |
| 16 | 01/08/23 | £300 | Card |
| 17 | 01/08/23 | £300 | Card |

| | | | |
|---|---|---|---|
| 18 | 01/08/23 | £300 | Card |
| 19 | 01/08/23 | £300 | Card |
| 20 | 01/08/23 | £300 | Card |
| 21 | 02/08/23 | £100 | Card |
| 22 | 02/08/23 | £100 | Card |
| 23 | 03/08/23 | £30 | Card |
| 24 | 03/08/23 | £300 | Card |
| 25 | 03/08/23 | £300 | Card |
| 26 | 03/08/23 | £300 | Card |
| 27 | 03/08/23 | £120 | Card |
| 28 | 11/08/23 | £1,500 | Transfer |
| 29 | 11/08/23 | £3,600 | Transfer |
| 30 | 12/08/23 | £1,900 | Transfer |
| 31 | 14/08/23 | £3,000 | Transfer |
| 32 | 18/08/23 | £8,000 | Transfer |
| 33 | 22/08/23 | £2,000 | Transfer |
| 34 | 29/08/23 | £5,000 | Transfer |
| 35 | 29/08/23 | £4,500 | Transfer |
| | *06/09/23* | *£5,500* | *Transfer-cancelled* |
| 36 | 06/09/23 | £3,000 | Transfer |
| 37 | 11/09/23 | £2,900 | Transfer |

Mr K says he could see his profits grow on a platform. He spoke to X's representative regularly and exchanged some emails. When he tried to withdraw funds Mr K realised he was the victim of a scam. His representative sent a letter of complaint to Wise in October 2023.

Wise didn't provide a final response but told this service why it was not reimbursing Mr K. In summary, Wise said:

- The account was registered on 27 June 2023 and Wise had no information about Mr K's income or usual account activity.
- The maximum amount Mr K paid to B was £2,000 in one day and the total amount was £4,715 over the period of a week. The transactions were low in value.
- Many customers use Wise accounts to buy cryptocurrency.
- The transfers were to accounts in Mr K's own name.
- While the warnings Wise gave to Mr K were generic, it was prevented from providing an investment warning because Mr K gave transfers to his own account as the payment reason and provided misleading responses to questions asked.
- It took proactive steps by pausing three transfers for additional verification. One of these payments was cancelled and returned to Mr K's account.

*Our investigation so far*

The investigator who considered this complaint recommended that it be upheld. He said that Wise should have intervened when Mr K made payment five on 27 July 2023 as it was the fourth payment to a cryptocurrency provider that day. Had Wise intervened, the investigator said that Mr K's loss would have been prevented. But Mr K should share the responsibility for his loss from this point, as there were scam warnings about X at the time, Mr K had no documentation, and didn't complete any research.

Mr K accepted the investigator's findings, but Wise did not so Mr K's complaint has been passed to me to decide. In summary, Wise said:

- All transfers were to Mr K's own accounts and its concerns were around safe account scams or account takeover. There were no suspicions of an investment scam.
- It acknowledges its responsibility to intervene and ask relevant questions, but it can't be held responsible when a customer provides misleading responses. Mr K said the funds were being transferred for a holiday. Given this, it is likely he wouldn't have told Wise the real reason for a payment if it had intervened earlier. And at that stage, Mr K thought the investment opportunity was legitimate so a tailored warning wouldn't have stopped him from making further payments.
- Wise does not have the ability to pause, suspend, or show warnings for outbound card payments in the same way it does for transfers. If a card payment is potentially fraudulent Wise can't reject it.
- Wise repeated the points it made when it submitted its file (which I have already set out above).

I intended to reach a different outcome to the investigator so issued a provisional decision on 30 June 2025. In the "What I've provisionally decided – and why" section of my provisional decision I said:

*I've considered all the available evidence and arguments to decide what's fair and reasonable in the circumstances of this complaint.*

*In deciding what's fair and reasonable, I am required to take into account relevant law and regulations, regulators' rules, guidance and standards, and codes of practice; and, where appropriate, I must also take into account what I consider to have been good industry practice at the time.*

*In broad terms, the starting position at law is that an Electronic Money Institution ("EMI") such as Wise is expected to process payments and withdrawals that a customer authorises it to make, in accordance with the Payment Services Regulations (in this case the 2017 regulations) and the terms and conditions of the customer's account.*

*Looking at what is fair and reasonable on the basis set out at DISP 3.6.4R, I consider that Wise should in July, August and September 2023 have been on the look-out for the possibility of fraud and have taken additional steps, or made additional checks, before processing payments in some circumstances.*

*Overall, taking into account relevant law, regulators rules and guidance, relevant codes of practice and what I consider to have been good industry practice at the time, I consider it fair and reasonable that Wise should:*

- *have been monitoring accounts and any payments made or received to counter various risks, including preventing fraud and scams;*
- *have had systems in place to look out for unusual transactions or other signs that*

*might indicate that its customers were at risk of fraud (among other things). This is particularly so given the increase in sophisticated fraud and scams in recent years, which firms are generally more familiar with than the average customer;*

- *from 31 July 2023 have acted to avoid causing foreseeable harm to customers, for example by maintaining adequate systems to detect and prevent scams and by ensuring all aspects of its products, including the contractual terms, enabled it to do so;*
- *in some circumstances, irrespective of the payment channel used, have taken additional steps, or made additional checks, or provided additional warnings, before processing a payment – (as in practice Wise sometimes does); and*
- *have been mindful of – among other things – common scam scenarios, how the fraudulent practices are evolving (including for example the common use of multi-stage fraud by scammers, including the use of payments to cryptocurrency accounts as a step to defraud consumers) and the different risks these can present to consumers, when deciding whether to intervene.*

*Should Wise have recognised that Mr K was at risk of financial harm from fraud?*

*It isn't in dispute that Mr K has fallen victim to a cruel scam here, nor that he authorised the payments he made by transfers to his cryptocurrency wallet (from where that cryptocurrency was subsequently transferred to the scammer) or to other accounts in his name.*

*I'm aware that cryptocurrency exchanges generally stipulate that the card used to purchase cryptocurrency at its exchange must be held in the name of the account holder, as must the account used to receive cash payments from the exchange. So Wise likely thought the transactions I have set out in the table above would be credited to a cryptocurrency account in Mr K's own name.*

*But by the time these payments were made, firms like Wise had been aware of the risk of multi-stage scams involving cryptocurrency for some time. Scams involving cryptocurrency have increased over time. The FCA and Action Fraud published warnings about cryptocurrency scams in mid-2018 and figures published by the latter show that losses suffered to cryptocurrency scams have continued to increase since. They reached record levels in 2022. During that time, cryptocurrency was typically allowed to be purchased through many high street banks with few restrictions.*

*So, taking into account all of the above I am satisfied that by the end of 2022, prior to the payments Mr K made, Wise ought fairly and reasonably to have recognised that its customers could be at an increased risk of fraud when using its services to purchase cryptocurrency, notwithstanding that the payment would often be made to a cryptocurrency wallet in the consumer's own name.*

*In those circumstances, as a matter of what I consider to have been fair and reasonable and good practice, Wise should have had appropriate systems for making checks and delivering warnings before it processed such payments. And, as I've set out, the introduction of the FCA's Consumer Duty, on 31 July 2023, further supports this view. The Consumer Duty requires Wise to avoid causing foreseeable harm to its customers by, among other things, having adequate systems in place to detect and prevent scams.*

*Taking all of the above into account, and in light of the increase in multi-stage fraud, particularly involving cryptocurrency, I don't think that the fact payments were going to an account held in Mr K's own name should have led Wise to believe there wasn't a risk of fraud.*

*I've gone on to consider, taking into account what Wise knew about the payments, at what point, if any, it ought to have identified that Mr K might be at a heightened risk of fraud.*

*I recognise that Mr K opened his Wise account on 27 June 2023 so Wise had little information about his usual account activity. But, as I have said above, I consider that by the time Mr K made these payments Wise should have recognised that cryptocurrency related transactions carry an elevated risk that the transaction is related to a fraud or scam. It's arguable that Wise should have intervened when Mr K made payment seven in the table above. Whilst the value of each transaction was low, and the overall amount paid wasn't at a level where I'd usually expect Wise to have concerns, Mr K had made multiple cryptocurrency related payments on the same day. Transaction seven was the sixth payment of £300 (to an identifiable provider of cryptocurrency) on the same day. This can be an indication of a deliberate attempt to bypass a firm's security systems and ensure payments are processed.*

*<u>What did Wise do to warn Mr K?</u>*

*Wise didn't provide any warnings in respect of any of the card payments. It says this is because all card payments received 3DS approval and the value of the transactions was low (with the maximum amount in one day being £2,000 spread over multiple payments and the total of all card payments being under £5,000). Wise also pointed out that many customers use its accounts to make cryptocurrency payments given the restrictions imposed by many banks.*

*Wise says that it provided a scam warning in respect of five of the transfers Mr K made. I have set out below the warning messages Wise provided:*

*"This could be a scam. Tell us what the transfer is for, and we can give you advice."*

*On each occasion, Mr K chose the 'Sending money to yourself' option and was required to answer the following questions,*

*"Has someone told you to move money because your account's at risk?*
*Is someone rushing or pressuring you to make this transfer?"*

*He gave a negative response to both questions and was shown a screen which said:*

*"New types of scams happen all the time. And it's hard to get your money back once you send it.*

*So, while your answers don't suggest this is a common scam, talk to someone you trust first. A second opinion can help you send safely."*

*Beneath this there was an option to click a link to find out more about scams.*

*Wise also paused three transfers for additional security checks. On 18 August 2023 Mr K was asked to provide a selfie holding an ID document and a copy of a recent statement to confirm that he was making the payment. Wise requested similar information on 6 September 2023 for a payment that was then cancelled. Later that day Mr K set up a transfer to his bank account and was asked to provide a photo of himself holding an ID document and the reason for the transfer. Mr K provided an email response in which he said it would be used for holidays.*

*What kind of warning should Wise have provided to Mr K?*

*I've thought carefully about what a proportionate warning in light of the risk presented by payment seven would be in these circumstances. In doing so, I've taken into account that many payments that look very similar to this one will be entirely genuine. I've given due consideration to Wise's duty to make payments promptly, as well as what I consider to have been good industry practice at the time this payment was made.*

*As I've set out above, the FCA's Consumer Duty, which was in force at the time most of these payments were made, requires firms to act to deliver good outcomes for consumers including acting to avoid foreseeable harm. In practice this includes maintaining adequate systems to detect and prevent scams and to design, test, tailor and monitor the effectiveness of scam warning messages presented to customers.*

*I think that by August 2023 Wise should have had systems in place to identify, as far as possible, the actual scam that might be taking place by asking automated questions. It should then have provided tailored warnings relevant to that scam for both APP and card payments.*

*I have considered Wise's points about its ability to pause or suspend card payments. The main card networks, Visa and Mastercard, don't allow for a delay between receipt of a payment instruction and its acceptance: the card issuer has to choose straight away whether to accept or refuse the payment. They also place certain restrictions on their card issuers' right to decline payment instructions. The essential effect of these restrictions is to prevent indiscriminate refusal of whole classes of transaction, such as by location. The network rules did not, however, prevent card issuers from declining particular payment instructions from a customer, based on a perceived risk of fraud that arose from that customer's pattern of usage. So it was open to Wise to decline card payments where it suspected fraud.*

*I've thought about what Mr K would have told Wise if it had asked questions to identify the potential scam risk as I think it should have. On all occasions when Mr K was asked for the reason for any payment to B, he said he was sending money to himself. Whilst this wasn't incorrect, as the account with B was in his name, there was a more obvious payment reason in the drop-down list Wise provided of investment.*

*I think it's more likely than not Mr K would have done the same thing in respect of this transaction and said he was sending money to himself. This means that the questions Wise would have asked Mr K would have been based on this payment purpose. Such questions would likely have covered whether he had been told his account wasn't safe and whether anyone had put pressure on him to make the payment quickly. Mr K had previously answered questions like these negatively.*

*I appreciate that Wise could have seen that the payment was going to a provider of*

*cryptocurrency. Given this, I consider Wise should have asked Mr K automated questions to establish which cryptocurrency scam he was most likely falling victim to (and then provided a tailored warning). I'm not persuaded Mr K would have told Wise that he was being instructed to move the funds by someone else, or that he was moving them on from his account at B on the instructions of a third-party, or that he was expecting to receive substantial profits. He later told his bank that nobody had approached him about the payment being discussed and I think he'd have answered similar questions in the same way. Wise should then have provided a written warning tailored to cryptocurrency investment scams.*

*I'm not persuaded that a written warning as set out above would have resonated with Mr K and prevented his loss, especially as he didn't heed verbal advice he was given at a later stage. Mr K was clearly under the spell of the scammer and was following the advice he was given. He had been communicating with her since June 2023, had opened multiple accounts on her instructions and took all steps requested by the scammer. On balance, I'm persuaded that Mr K would have gone ahead with the transaction after seeing a written warning. I will add that I do not believe Wise needed to go further than to provide an on-screen warning at this stage.*

*Mr K then made multiple transfers to an account in his own name with Z. Whilst Wise might have been reassured by the fact the transfers were to an account in his name, I think it ought reasonably to have intervened when Mr K made payment 32 in the table above (on 18 August 2023). I think Wise should have asked some questions to understand the reason for the payment and to satisfy itself Mr K wasn't at risk of financial harm. I say this given the pattern of increasing payments to Z and the fact they follow a series of cryptocurrency related payments.*

*Wise did pause this payment, but it only asked for verification information and didn't ask anything about the reason for the payment. I don't consider it went far enough.*

*I've thought carefully about what would have happened if Wise had intervened as I think it should have. I have received very limited information from Mr K about the scam. It appears that much of his communication with the scammer was by phone and there were some emails. Based on the available evidence, I'm not persuaded it's more likely than not that intervention of the type described would have prevented Mr K's further losses. In saying this, I have been guided by the information Mr K provided when Wise and other firms interacted with him.*

*On 6 September 2023, Mr K responded to Wise by email and said that a transaction it had highlighted was for a holiday. Then on 11 September 2023, he told his bank in a call that a transaction it blocked, and others, related to a trip abroad to see family. Mr K said that he hadn't been on holiday for six years and wanted to spoil the family by buying appliances and gifts for his grandchildren. Mr K also confirmed that no-one had approached him, and he hadn't been coerced.*

*Finally, I'm aware that on 20 September 2023 another bank blocked a £9,000 payment. The third-party bank has not provided me with a call recording but has agreed to provide some information. Mr K told this bank that the payment was for a holiday abroad and for flights. His bank had concerns that he was being coerced into making the payment and gave him advice about investment scams, impersonation scams and remote access scams. Mr K confirmed that he wasn't being coerced but his bank declined the payment. The following day, Mr K made the payment from another account, demonstrating just how involved in the scam he was.*

*Having considered the interactions Mr K had with Wise and two other banks, I'm persuaded that he would have misled Wise about the real reason for payment 32. I recognise this was likely because he was being coached, but I'm not persuaded I can reasonably conclude that Wise could have uncovered the scam.*

*Overall, whilst I'm very sorry to hear about this cruel scam, I can't fairly hold Wise liable.*

Responses to my provisional decision

Wise didn't respond to my provisional decision.

Mr K, through his professional representative, didn't agree with my provisional findings. In summary, he said that Wise's interventions weren't sufficient, and that better intervention would have uncovered the scam. The main points Mr K made are set out below:

- Automated questions would not have been sufficient given Mr K's age and that he made payments for cryptocurrency from a newly opened account. He said Wise needed to speak to him, particularly given that scam victims are often asked to open new EMI accounts.
- Banks and EMIs shouldn't accept the answers given in response to fraud queries at face value, especially in respect of the payment purpose, given that victims are often coached.
- The reasons Mr K might have given for the payments, like a holiday and buying appliances and gifts for his grandchildren should have led to greater scrutiny. For example, Mr K should have been asked why he had moved funds to a new EMI account for these purposes.
- Moving funds into an account and then on from that account quickly is a clear sign of multi-stage fraud that Wise should have picked up on.

To support some of these points Mr K's representative has quoted from previous decisions issued by this service.

**What I've decided – and why**

I've considered all the available evidence and arguments to decide what's fair and reasonable in the circumstances of this complaint.

I have carefully considered Mr K's response to my provisional decision but am not persuaded to change it. My final decision is the same as my provisional (which I have reproduced above), and for the same reasons.

I consider that Wise ought reasonably to have recognised an increased risk of harm when Mr K made payment seven. It should have asked a series of automated questions to understand the reason for the payment before providing a warning tailored to that payment reason. I'm not persuaded such a warning would have resonated with Mr K or prevented the payment from being made. By payment 32 I consider Wise should have asked Mr K questions. But, given the interventions of third parties, I'm not satisfied such intervention would have made a difference.

I don't accept that a proportionate response to the risk posed by payment seven would have been to speak to Mr K. The account was newly opened so Wise didn't have information to understand Mr K's usual spending habits. The payments he made up to this point were very low value and weren't increasing in value. But, because Mr K made a series of payments from this new account on the same day to an identifiable provider of cryptocurrency, I think

Wise should fairly and reasonably have taken steps to identify the reason for the payment and then to have given a tailored warning.

I turn now to what is most likely to have happened if Wise had intervened when Mr K made transaction 32. I agree that banks and EMIs shouldn't take all answers given in response to fraud screening questions at face value. But I'm not persuaded that Mr K would have revealed the true reason for the payment if Wise had asked probing questions. In saying this I have considered what happened when two other banks intervened, and spoke to Mr K, when he made transactions as part of the same scam. Mr K told both banks that transactions related to a holiday abroad and referred to buying electrical items and gifts for grandchildren. Given the nature of the service provided by Z I don't think Wise would have been concerned by such responses.

I also agree that Wise could have asked why Mr K chose to use Z rather than Wise, given that they offer broadly similar services. But I think Mr K could easily have responded to such a question as exchange rates vary between the firms and there may have been other reasons why Mr K decided to use Z rather than Wise.

Mr K's representative has quoted from various decisions previously issued by this service. We consider each case on its own merits, and there is no context or information about the circumstances of each case referred to.

Overall, whilst I'm very sorry Mr K has fallen victim to this scam and lost a substantial amount of money, I can't fairly require Wise to reimburse him.

**My final decision**

For the reasons stated, I do not uphold this complaint.

Under the rules of the Financial Ombudsman Service, I'm required to ask Mr K to accept or reject my decision before 11 August 2025.

Jay Hadfield
**Ombudsman**